

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Previously Presented) An intrusion secure personal computer system comprising:
 - a central processing unit;
 - a data storage means;
 - a memory means;
 - a primary operating system;
 - a virtual machine operating system providing an isolated secondary operating environment functioning separate from the primary operating system and controlling operations of the personal computer system within the isolated secondary operating environment; and
 - at least one input/output (I/O) connection in operative communication with an external data source,wherein the personal computer system is secured from malicious code contained in a file downloaded from the external data source.
2. (Previously Presented) The computer system of claim 1, wherein the external data source is a global computer network.
3. (Canceled)
4. (Previously Presented) The computer system of claim 1, wherein the external data source is at least one external data source selected from the group consisting of: a computer workstation, a personal-type computer, a computer dock, a local area network, an intranet, and a wide area network.
5. (Previously Presented) The computer system of claim 1, wherein the virtual machine operating system comprises software for defining a virtual machine environment in memory and a virtual drive in storage, and operational control software limiting operative communication with the external data source to the virtual machine environment and the virtual machine drive.

6. (Currently Amended) A method for securing a personal computer system from intrusion from an external data source comprising the steps of:

providing an intrusion secure personal computer system ~~of claim 1~~ comprising:

a central processing unit;

a data storage means;

a memory means;

a primary operating system;

a virtual machine operating system providing an isolated secondary operating environment functioning separate from the primary operating system and controlling operations of the personal computer system within the isolated secondary operating environment; and

at least one input/output (I/O) connection in operative communication with an external data source,

wherein the personal computer system is secured from malicious code contained in a file downloaded from the external data source;

initiating an external data source interface session, wherein initiating the external data source interface session causes activation of a the virtual machine operating system ~~of claim 1~~ and defines a virtual machine environment in memory and a virtual drive in storage; and

establishing connectivity with the external data source under control of the virtual machine operating system to isolate operative communication with the external data source to the virtual machine environment and the virtual drive to secure the computer system from intrusion from the external data source.

7-25. (Canceled)

26. (Previously Presented) A security method for protecting a personal computer from malicious code derived from an external data source comprising the steps of:

loading a software application installable on the personal computer, wherein the software application protects the personal computer's primary data files from being accessed by malicious code from the external data source;

installing the software application on the personal computer, the installed application defining an isolated operating environment including a secondary operating system, the secondary operating system functioning in conjunction with and separate from a primary operating system on the personal computer, and the installed application defining primary operating system permission codes to limit access to a node connectable to the external data source to the isolated operating environment under control of the secondary operating system;

initiating an external data source interface session via the node within the isolated operating environment, and allocating a volatile memory space and a temporary data storage space to the secondary operating system for the duration of the session; and

establishing connectivity with the external data source via the node under control of the secondary operating system to isolate operative communication with the external data source to the isolated operating environment, and protecting the personal computer from malicious code derived from the external data source.